A

I - zamki elektroniczne II zamki cyfrowe

Ulica Kluczborska 2.11.2018 godz 19.00

| Rower | Kod z aplikacji | Kod na zamku | Typ |
|---|---|---|---|
| 57238 | 5169 | 2526 | II |
| 57046 | 5341 | 5541 | I |
| 57985 | 4232 | 4245 | I |
| 57878 | 6621 | 8852 | II |
| 57249 | 4371 | 2359 | II |
| 57519 | 1409 | 1515 | I |
| 57022 | 4839 | 4395 | II |
| 57510 | 9728 | 979* | II |
| 57435 | 9975 | **74 | II |

Ulica Strachocińska 3.11.2018 godz 20.00

| Rower | Kod z aplikacji | Kod na zamku | Typ |
|---|---|---|---|
| 57092 | 8407 | 9629 | I |
| 57572 | 3561 | 1772 | I |
| 57532 | 4556 | 3*14 | I |
| 57066 | 7942 | 7945 | I |

| | | | |
|---|---|---|---|
| 57201 | 4216 | 31*5 | I |
| 57087 | 8760 | 8769 | I |
| 57154 | 9228 | 36*4 | I |

Teki 3.11.2018 godz 20.30

| Rower | Kod z aplikacji | Kod na zamku | Typ |
|---|---|---|---|
| 63734 | 4658 | 2228 | I |
| 57451 | 5922 | 5799 | I |
| 57526 | 2219 | 5759 | I |
| 57460 | 2527 | 4858 | II |
| 57851 | 8787 | 8789 | II |
| 57946 | 6627 | 7244 | II |
| 57935 | 5553 | 5555 | I |
| 57907 | 4370 | 4377 | I |
| 57380 | 9924 | 9923 | I |

Ulica Wesoła 4.11.2018 00.50

| Rower | Kod z aplikacji | Kod na zamku | Typ |
|---|---|---|---|
| 57775 | 1429 | 1529 | II |
| 57417 | 6829 | 6719 | II |

| | | | |
|---|---|---|---|
| 57070 | 9634 | 9271 | II |

| | | | |
|---|---|---|---|
| 57378 | 1744 | 1844 | II |

| | | | |
|---|---|---|---|
| 57564 | 9966 | 9136 | II |

Dodatkowy wynik:

| | | | |
|---|---|---|---|
| 57197 | 6332 | 6330 | II |

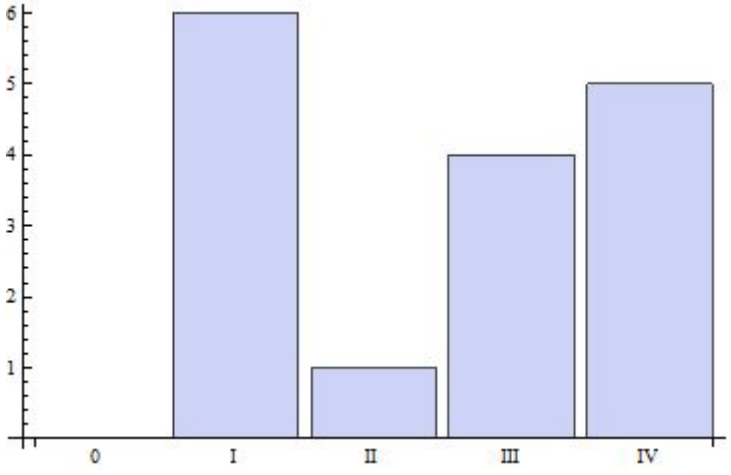
* oznacza dodatkowy znak pomiędzy 9 a 1.

B

Wykresy rozkładów według kategorii jak bardzo różni się kod z aplikacji od tego zastanego na zamku szyfrowym

Kategoria(0)- niczym się nie różnią
Kategoria (I) - różnią się tylko na jednej pozycji
Kategoria(II) - różnią się na dwóch pozycjach.
Kategoria (III) -różnią się na trzech pozycjach.
Kategoria (IV) -różnią się na czterech pozycjach.

Rozkład dla zamka elektronicznego :

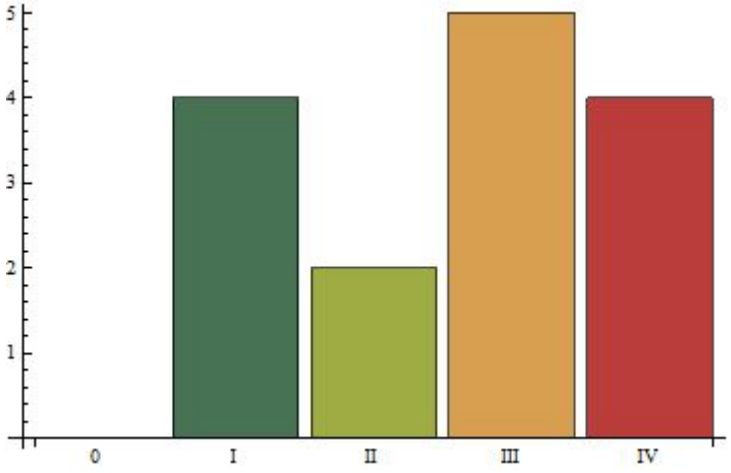


Entropię obliczamy ze wzoru

$$entropia(Dane) = I(Dane) = -\sum_{i=1}^{k} P(wartosc_i) * log_2(P(wartosc_i))$$

$$I(kategora\ I) = -[(\tfrac{6}{16})log_2(\tfrac{6}{16}) + (\tfrac{1}{16})log_2(\tfrac{1}{16}) + (\tfrac{4}{16})log_2(\tfrac{4}{16}) + (\tfrac{5}{16})log_2(\tfrac{5}{16})] = 1.805036$$

Rozkład dla zamka cyfrowego :




$$I(kategoria\ II) = -[(\tfrac{4}{15})log_2(\tfrac{4}{15}) + (\tfrac{2}{15})log_2(\tfrac{2}{15}) + (\tfrac{5}{15})log_2(\tfrac{5}{15}) + (\tfrac{4}{15})log_2(\tfrac{4}{15})] =$$
= 1.84706

Różnice mogą się brać z większej ilość szyfrów z gdzie 2 pozycje są zmienione.
Jak widać w jednym i drugim najmniej jest haseł które różnią się na 2 pozycjach .
W przypadku zamka elektronicznego jest więcej haseł z gdzie tylko jedna litera jest przestawiona.

C Entropia hasła mierzy jak bardzo nieprzewidywalne jest hasło

Można ją obliczać wzorem $E = log_2(R^L)$ gdzie
$E$ - entropia hasła
$R$ - moc alfabetu z którego składa się hasło
$L$ - długość hasła
$R^L$ - wszystkie możliwe hasła od długości L nad danym alfabetem
$log_2(R^L)$ - liczba bitów entropii

Hasło jest cięższe do złamania im większe jest E.

Dla 4 cyfrowych pinów gdzie alfabet wynosi od 0-9 otrzymamy 13 bit entropii

Dla 8 cyfrowych PIN-ów entropia wynosi  26 bitów a z alfabetem alfanumerycznym (36 znaków) entropia wynosi 41 bitów. Nie wiele podniesie to bezpieczeństwo gdy użytkownicy będą zmieniać zamek o 1 pozycję.

2 . Rozkłady dla poprawnych danych powinne być  przybliżone, entropie także